Always CHECK before you CLICK! Don’t help others steal your information.

TARGETED EMAILS from hackers will look legitimate at first glance

Make sure the email is GENUINE before you click on any links!

What To Check For

1. Look for unprofessional spelling or grammar errors.

2. Treat any email you didn’t expect to receive with suspicion.

3. Check for odd phrases and word choice based on your knowledge of the sender.

4. Hover over links to see if the web address is legitimate and relates to the email’s content.

5. Verify any email that asks for personal information by independently looking up the sender’s contact information.

Learn more at security.ucop.edu